Explain the term “critical infrastructure” in your own words and give real-life examples for critical infrastructures.

Critical infrastructure is a term used for organisations/assets that are of great importance for general life or that are essential for the functioning of the society. Infrastructure is considered “critical” when any failure of the infrastructure would result in severe supply bottlenecks, significant disruption to public safety or other dramatic consequences. Regarding their technical, structural, and functional specifics, critical infrastructures can be classified in to two, technical basic infrastructure and socio-economic services infrastructure.

**Technical basic infrastructure includes.**

Transport and traffic

Sewage and drinking water supply

Power supply

IT and telecommunication

**Socio-economic services infrastructure includes.**

Parliament and government administrative institutions

Rescue services and disaster control

Financial sector (Banks, Stock exchange, Insurance)

Medical care

Judicial Institutes

Culture and media sector

What legal requirements are stated for companies operating critical infrastructures? Hint: Refer to the exercise sheet and surf the web!

To protect the public, critical infrastructures’ functionality should be maintained as far as possible in the event of emergency. Therefore, there are some legal requirements, in respect to the operator’s needs, that must be abided by the operator.

**The European Programme for Critical Infrastructure Protection (EPCIP**) refers to the doctrine and programmes created to identify and protect critical infrastructure that, in case of fault, incident or attack can be protected.

In particular, operators of Critical Infrastructure will have to (a) implement state of the art technical and organizational measures and (b) notify the regulator in case of security incidents.

**(a) Technical and Organizational Measures\*\***

* Operators of Critical Infrastructure must implement state of the art technical and organizational to prevent disturbances of any kind
* For the sectors Energy, Information Technology and Telecommunications, Water and Food, respective measures must generally be implemented until May 2018 at the latest
* For the sectors Transport and Traffic, Health as well as Finance and Insurance, an administrative decree will specify which specific operators will be considered to provide “Critical Infrastructures”; from the date of such decree on (which is expected to be passed until the end of 2016), the operators have to implement the necessary measures within a time frame of two years
* Operators must demonstrate every two years that their security measures are state of the art
* Industry Associations may elaborate industry security standards; the responsible regulator can confirm that these standards are sufficient

**(b) Notification Requirements\*\***

Operators of Critical Infrastructure must

* Designate single points of contacts for communication with competent authorities until November 2016
* Notify the responsible regulator in case of significant incidents affecting the availability, integrity, authenticity and confidentiality of its IT systems, components and processes that could lead or have led to an outage or impairment of critical infrastructure; notifications can be submitted on an anonymized basis unless an outage or impairment has indeed occurred

**(c) Obligations for specific energy and telecom providers\*\***

* In addition, there had already been pre-existing IT security standards in highly regulated parts of the industries of energy (e.g. operators of atomic plants) and telecom. For those sectors, the IT Security Law holds additional IT security requirements and notification obligations. In addition, operators of energy grids will have to implement an Information Security Management System (ISMS) consistent with ISO/IEC 27001.

**(d) Enforcement\*\***

* Authorities can impose fines of up to 100,000 € if operators do not comply with binding orders to remedy their operations
* In other cases, such as failure to provide information on the implementation of security measures or failure to notify incidents, fines can be as high as 50,000 €
* In addition, other consequences such as damage claims may arise in case of non-compliance

Legal laws in Germany pertaining to critical infrastructures:

* Act on the Federal Office for Information Security (BSIG)
* Atomic Energy Act (AtG)
* Energy Industry Act (Energy Industry Act (EnWG)
* Telemedia Act (TMG)
* Telecommunications Act (TKG)
* Act on the Federal Criminal Police Office (BKAG)

Give some example statements for the overall security policy (cf. ISO27k2, A.5.1.1) related to the chosen CRITIS.

Overall Security policy

High level

* Significance of Information security in eHealth is immense to protect vital assets against cyber threats.
* ISMS provide security risk assessment and secures processing of eHealth systems to ensure continuity without interruption by internal or external threats.
* Objective of our policy is to protect the Hospital’s information assets through safeguarding its confidentiality, integrity, and availability
* CISO should assign security management roles and the ISO’s or Area specific managers should ensure the implementation of the security policy.
* The security policy should be reviewed and improved by the Information security Committee to ensure security needs of changing times.

Low Level

* Access control: Controls applied to Authorized personnel must be more comprehensive than for other users.
* Backup: Comprehensive information and system backup procedures and archiving MUST be implemented.
* Physical Security: Building and entry controls for areas used in the processing and storage of security classified information must be established and maintained.
* Network Security: Network must be segregated and scanned to ensure that traffic entering and leaving the agency network malicious free.
* Business Continuity: Business continuity plans MUST be maintained and tested to ensure information and eHealth assets are available and consistent with Hospital’s business and service level requirements.
* Protection from Malware: Adequate controls MUST be defined and implemented for the prevention, detection, removal and reporting of attacks by malicious code on all Information assets.
* Information Classification: All information assets must be assigned appropriate security classification in accordance with criticality or vulnerability to threats.
* Management of Technical Vulnerabilities: A patch management program for operating systems, firmware and applications of all information assets MUST be implemented to maintain vendor support, increase stability, and reduce the likelihood of threats being exploited.

These security policies should be conveyed to employees and relevant external parties that is easily accessible and understandable to the intended user.

Describe the business model of the critical infrastructure you have selected and describe the 10 most important business critical assets. Give as many technical details as possible: servers, clients, special devices (smart meter, mobile apps for patients), network topology.

**BUISNESS MODEL “E-health”**

**ASSETS**

* Health Information systems, i.e. the information networks in the hospitals.
* Clinical data repositories i.e. the databases in each hospital where information is stored locally.
* Authentication server i.e. to perform access control and authentication of users.
* Laboratory Information System (LIS).
* Radiology Information Systems (RIS).
* Picture Archiving and Communication Systems (PACS), i.e. transferring radiology results.
* Electronic Health Record components.
* Patient Health Record service.
* E-Prescription service.